PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-305853
(43)Date of publication of application : 02.11.2000

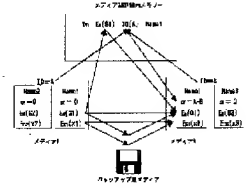
(51)Int.Cl. G06F 12/14
// G09C 1/00

(21)Application number : 11-114661
(22)Date of filing : 22.04.1999

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : SUGAWARA TAKAYUKI
HIRATA ATSUMI

(54) METHOD FOR RECORDING CONTENTS INFORMATION AND CONTENTS INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To make it possible to transfer a medium in which contents information is recorded between users while preventing the occurrence of illegal copying.
SOLUTION: In the case of transferring ciphered contents information EG1(x1) from a medium A to a medium B, cipher key information EA(G1) and the ID(A) of the medium A are recorded in a memory built in a medium controller as the management number Dn of data link ID. The number Dn is added to the information EG1(x1) and copied in the medium B together with the information EA(G1). The EA(G1) read out from the medium B is collated with the EA(G1) read out from the memory, and when the EA(G1) is matched with the EA (G1), a difference ID(A-B) value as a difference between the ID of the medium B and that of the medium A is outputted to the medium B. After outputting the difference ID(A-B) value, the EA(G1) and the ID(A) recorded in the memory are erased.



LEGAL STATUS

[Date of request for examination] 30.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－305853
（Ｐ２０００－３０５８５３Ａ）
(43)公開日　平成12年11月２日(2000.11.2)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ			テーマコード（参考）
G06F 12/14	320	G06F 12/14	320	E	5B017
			320	B	5J104
// G09C 1/00	660	G09C 1/00	660	G	
			660	D	

審査請求　未請求　請求項の数15　ＯＬ　（全18頁）

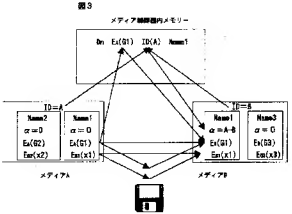
(21)出願番号　特願平11－114661
(22)出願日　平成11年４月22日(1999.4.22)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　菅原　隆幸
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(72)発明者　平田　潤美
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Ｆターム(参考)　5B017 AA06 BA05 BA07 BB03 CA06 CA07 CA09 CA16
5J104 AA01 AA07 JA03 JA21 KA02 NA02 NA05 NA31 PA14

(54)【発明の名称】コンテンツ情報記録方法及びコンテンツ情報処理装置

(57)【要約】
【課題】　不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡可能とする。
【解決手段】　メディアAからメディアBに暗号化コンテンツ情報EG1(X1)を譲渡する場合、暗号化鍵情報EA(G1)とメディアAのID(A)とはメディア制御器のメモリーにデータリンクIDの管理ナンバーDnとして記録される。EG1(X1)にはDnが付加されてEA(G1)と共にメディアBにコピーされる。メディアBから読み出したEA(G1)とメモリーから読み出したEA(G1)とを照合し一致している場合、メディアBとメディアAのIDの差分値である差分ID（A-B）値を、メディアBに出力する。出力後、メモリーに記録されているEA(G1)とID（A）を消去する。



1

【特許請求の範囲】

【請求項１】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコンテンツ情報記録方法であって、

前記第１のメディアのメディアＩＤに関する情報を前記第１及び第２のメディア以外の所定のメモリに一時記録して、前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、

前記第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから形成される独自１ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去することを特徴とするコンテンツ情報記録方法。

【請求項２】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコンテンツ情報記録方法であって、

前記第１のメディアのメディアＩＤに関する情報をデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所定のメモリに一時記録し、

前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、

前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを得、

前記第２のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その２つの暗号化鍵情報が一致しているときのみ、前記第２のメディアのメディアＩＤに関する情報と前記メモリから読み出した前記第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを消去することを特徴とするコンテンツ情報記録方法。

【請求項４】前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、

前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であることを特徴とする請求項１～３のいずれか一つに記載のコンテンツ情報記録方法。

【請求項５】前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であることを特徴とする請求項１～４のいずれか一つに記載のコンテンツ情報記録方法。

【請求項６】前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ＩＤ鍵は、第１のメディアのメディアＩＤを用いた共通鍵または第１のメディアのメディアＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とする請求項１～５のいずれか一つに記載のコンテンツ情報記録方法。

【請求項７】第１のメディアのメディアＩＤに関する情報を一時記録するメモリと、

第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、この独自ＩＤ情報を第２のメディアに記録する独自ＩＤ情報形成手段と、

前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消

2

去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項８】前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、

前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であることを特徴とする請求項７に記載のコンテンツ情報処理装置。

【請求項９】前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であることを特徴とする請求項７または８に記載のコンテンツ情報処理装置。

【請求項１０】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する際の前記各メディアのＩＤに関する情報を処理するコンテンツ情報処理装置であって、

前記第１のメディアのメディアＩＤに関する情報を一時記録するメモリと、

前記第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、前記暗号化コンテンツ情報と前記暗号化鍵情報とが前記第２のメディアに記録された後に、前記独自ＩＤ情報を前記第２のメディアに記録する独自ＩＤ情報形成手段と、

前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項１１】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する際の前記各メディアのＩＤに関する情報を処理するコンテンツ情報処理装置であって、

前記第１のメディアのメディアＩＤに関する情報をデータリンクＩＤによって対応づけられた形態で一時記録するメモリと、

前記データリンクＩＤを前記第１のメディアに記録するデータリンクＩＤ書き込み手段と、

前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとが前記第２のメディアに記録された後に、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報を得て、この第１のメディアのメディアＩＤに関する情報と前記第２のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、前記独自ＩＤ情報を前記第２のメディアに記録する独自ＩＤ情報形成手段と、

前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項１２】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する際の前記各メディアのＩＤに関する情報を処理するコンテンツ情報処理装置であって、

前記第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とをデータリンクＩＤによって対応づけられた形態で一時記録するメモリと、

前記データリンクＩＤを前記第１のメディアに記録するデータリンクＩＤ書き込み手段と、

前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとが前記第２のメディアに記録された後に、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記第２のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、前記独自ＩＤ情報を前記第２のメディアに記録する独自ＩＤ情報形成手段と、

前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

【請求項１３】前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、

前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であることを特徴とする請求項

１０～１２のいずれか一つに記載のコンテンツ情報処理装置。

【請求項１４】前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であることを特徴とする請求項１０～１３のいずれか一つに記載のコンテンツ情報処理装置。

【請求項１５】前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ＩＤ鍵は、第１のメディアのメディアＩＤを用いた共通鍵または第１のメディアのメディアＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とする請求項１０～１４のいずれか一つに記載のコンテンツ情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、これに使用したコンテンツ鍵に対してそのメディアのＩＤをＩＤ鍵として暗号化した暗号化鍵情報とを、記録再生するコンテンツ情報暗号化システムに関するものである。そして、この発明はコンテンツ情報（特にオーディオやビデオのデータ）を配信し、配信されたデータを不正なコピーを阻止しながら、ユーザーのメディア間でのデータの譲渡（移動）を安全に行うことのできるコンテンツ情報暗号化システムにおけるコンテンツ情報記録方法及びコンテンツ情報処理装置を提供することを目的としている。

【０００２】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのディジタルデータを配信する有用な方法として、特開平１０－２６９２８９号公報に記載のディジタルコンテンツ配布管理方法、ディジタルコンテンツ再生方法及び装置がある。この発明においては、ディジタルコンテンツの配布側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツに使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。また、特開平９－２５３０３号公報に記載の情報記録媒体、記録装置、情報伝送システム、暗号解読装置がある。この発明の情報記録媒体は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるにもかかわらず、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーし、不正使用をすることを防止した。

【０００３】

【発明が解決しようとする課題】しかしながら上記の従来の方式では、コンテンツデータの記録されたメディアを、ユーザー間で譲渡することが出来ない（メディア自体の譲渡はできてもそのメディアに記録されたコンテンツデータの正規の再生ができない。）ので、ユーザーがコンテンツデータを手に入れるためには、一度は必ず課金管理機関、データ管理センター等に接続しなければならない。また、１人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの移動や、一時バックアップをしてから、不正なコピーを防止しつつ、任意のメディアにデータを復帰させることができない。本発明は、コンテンツ情報を配信し、配信されたデータを不正なコピーを阻止しながら、ユーザーのメディア間でのデータの譲渡（移動）を安全に行うことのできるコンテンツ情報暗号化システムにおけるコンテンツ情報記録方法及びコンテンツ情報処理装置を提供することを目的としている。

【０００４】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記の方法、装置を提供するものである。

（１）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコンテンツ情報記録方法であって、前記第１のメディアのメディアＩＤに関する情報を前記第１及び第２のメディア以外の所定のメモリに一時記録して、前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、前記第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去することを特徴とするコンテンツ情報記録方法。

（２）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコ

ンテンツ情報記録方法であって、前記第１のメディアのメディアＩＤに関する情報をデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報を得て、この第１のメディアのメディアＩＤに関する情報と前記第２のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去することを特徴とするコンテンツ情報記録方法。

（３）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコンテンツ情報記録方法であって、前記第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とをデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを得、前記第２のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その２つの暗号化鍵情報が一致しているときのみ、前記第２のメディアのメディアＩＤに関する情報と前記メモリから読み出した前記第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを消去することを特徴とするコンテンツ情報記録方法。

（４）前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であることを特徴とする上記（１）～（３）のいずれか一つに記載のコンテンツ情報記録方法。

（５）前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であることを特徴とする上記（１）～（４）のいずれか一つに記載のコンテンツ情報記録方法。

（６）前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ＩＤ鍵は、第１のメディアのメディアＩＤを用いた共通鍵または第１のメディアのメディアＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とする上記（１）～（５）のいずれか一つに記載のコンテンツ情報記録方法。

（７）第１のメディアのメディアＩＤに関する情報を一時記録するメモリと、第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、この独自ＩＤ情報を第２のメディアに記録する独自ＩＤ情報形成手段と、前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

（８）前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であることを特徴とする上記（７）に記載のコンテンツ情報処理装置。

（９）前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であることを特徴とする上記（７）または（８）に記載のコンテンツ情報処理装置。

（１０）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する際の前記各メディアのＩＤに関する情報を処理するコンテンツ情報処理装置であって、前記第１のメディアのメディアＩＤに関する情報を一時記録するメモリと、前記第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、前記暗号化コンテンツ情報と前記暗号化鍵情報とが前記第２のメディアに記録された後に、前記独自ＩＤ情報を前記第２のメディアに記録する独自ＩＤ情報形成手段と、前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

（１１）所定のコンテンツ鍵で暗号化された暗号化コン

テンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する際の前記各メディアのＩＤに関する情報を処理するコンテンツ情報処理装置であって、前記第１のメディアのメディアＩＤに関する情報をデータリンクＩＤによって対応づけられた形態で一時記録するメモリと、前記データリンクＩＤを前記第１のメディアに記録するデータリンクＩＤ書き込み手段と、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとが前記第２のメディアに記録された後に、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報を得て、この第１のメディアのメディアＩＤに関する情報と前記第２のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、前記独自ＩＤ情報を前記第２のメディアに記録する独自ＩＤ情報形成手段と、前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

（１２）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する際の前記各メディアのＩＤに関する情報を処理するコンテンツ情報処理装置であって、前記第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とをデータリンクＩＤによって対応づけられた形態で一時記録するメモリと、前記データリンクＩＤを前記第１のメディアに記録するデータリンクＩＤ書き込み手段と、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとが前記第２のメディアに記録された後に、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを読み出すメモリ読み出し手段と、前記第２のメディアから読み出した前記暗号化鍵情報と、前記メモリ読み出し手段により前記メモリから読み出した前記暗号化鍵情報とを照合する暗号化鍵情報照合手段と、この暗号化鍵情報照合手段により前記２つの暗号化鍵情報が一致していると判断されたときのみ、前記第２のメディアのメディアＩＤに関する情報と前記メモリから読み出した第１のメディアのメディアＩＤに関する情報とから独自ＩＤ情報を形成して、前記独自ＩＤ情報を前記第２のメディアに記録する独自ＩＤ情報形成手段と、前記独自ＩＤ情報形成後に前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを消去する消去手段とを設けたことを特徴とするコンテンツ情報処理装置。

（１３）前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であることを特徴とする上記（１０）～（１２）のいずれか一つに記載のコンテンツ情報処理装置。

（１４）前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であることを特徴とする上記（１０）～（１３）のいずれか一つに記載のコンテンツ情報処理装置。

（１５）前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ＩＤ鍵は、第１のメディアのメディアＩＤを用いた共通鍵または第１のメディアのメディアＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とする上記（１０）～（１４）のいずれか一つに記載のコンテンツ情報処理装置。

【０００５】

【発明の実施の形態】本発明によれば、不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。また、本発明によれば、１人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの移動や、一時バックアップをしてから、不正なコピーを防止しつつ、任意のメディアにデータを復帰させるシステムを提供できる。

【０００６】本発明では、

［ａ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコンテンツ情報記録する場合に、前記第１のメディアのメディアＩＤに関する情報を前記第１及び第２のメディア以外の所定のメモリに一時記録して、前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第２のメディアに記録するとともに、前記第１のメディアから前記暗号化鍵情報を消去し、前記第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録するとともに、前記メモリ

リから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去するようにした。

［ｂ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録するコンテンツ情報記録場合に、前記第１のメディアのメディアＩＤに関する情報をデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報を得て、この第１のメディアのメディアＩＤに関する情報と前記第２のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去するようにした。

［ｃ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する場合に、前記第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とをデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを得、前記第２のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その２つの暗号化鍵情報が一致しているときのみ、前記第２のメディアのメディアＩＤに関する情報と前記メモリから読み出した前記第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを消去するようにした。

【０００７】［ｄ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する場合に、前記第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とをバックアップ用メディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、その後、前記バックアップ用メディアから前記暗号化コンテンツ情報と前記暗号化鍵情報とを前記第２のメディアに記録すると共に、前記第２のメディアのメディアＩＤに関する情報と前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録し、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去するようにした。

［ｅ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する場合に、前記第１のメディアのメディアＩＤに関する情報をデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとをバックアップ用メディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、その後、前記バックアップ用メディアから前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報を得て、この第１のメディアのメディアＩＤに関する情報と前記第２のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報を消去するようにした。

［ｆ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記暗号化コンテンツ情報が記録される第１のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報とを記録した前記第１のメディアから、前記暗号化コンテンツ情報と前記暗号化鍵情報とを第２のメディアに記録する場合に、前記第１のメディアのメディアＩＤに関する情報とデータリンクＩＤによって対応づけられた形態で前記第１及び第２のメディア以外の所

定のメモリに一時記録し、前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとをバックアップ用メディアに記録すると共に、前記第１のメディアから前記暗号化鍵情報を消去し、その後、前記バックアップ用メディアから前記暗号化コンテンツ情報と前記暗号化鍵情報と前記データリンクＩＤとを前記第２のメディアに記録すると共に、前記第２のメディアから読み出した前記データリンクＩＤを基に、前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを得、前記第２のメディアから読み出した前記暗号化鍵情報と前記メモリから読み出した前記暗号化鍵情報とを照合し、その２つの暗号化鍵情報が一値しているときのみ、前記第２のメディアのメディアＩＤに関する情報と前記メモリから読み出した前記第１のメディアのメディアＩＤに関する情報とから形成される独自ＩＤ情報を前記第２のメディアに記録すると共に、前記メモリから前記一時記録された第１のメディアのメディアＩＤに関する情報と前記暗号化鍵情報とを消去するようにした。

【０００８】［ｇ］前記メモリに一時記録された第１のメディアのメディアＩＤに関する情報が、前記第１のメディアから読み出された第１のメディアのメディアＩＤに基づく情報であり、前記第２のメディアのメディアＩＤに関する情報が、前記第２のメディアから読み出された第２のメディアのメディアＩＤに基づく情報であるようにした。

［ｈ］前記独自ＩＤ情報が、前記第１のメディアのメディアＩＤと前記第２のメディアのメディアＩＤとの差分値である差分ＩＤ情報であるようにした。

［ｉ］前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ＩＤ鍵は、第１のメディアのメディアＩＤを用いた共通鍵または第１のメディアのメディアＩＤを所定の関数により変換した情報を用いた共通鍵であるようにした。

【０００９】［ｊ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、他のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報と、前記他のメディアのメディアＩＤに関する情報と本メディアのメディアＩＤに関する情報とから形成された独自ＩＤ情報とが記録されたメディアからコンテンツ情報を復元する場合に、前記独自ＩＤ情報と前記本メディアのメディアＩＤとから前記他のメディアのメディアＩＤに関する情報を得て、前記暗号化鍵情報から前記コンテンツ鍵を復元し、このコンテンツ鍵を用いて前記暗号化コンテンツ情報を復元するようにした。

［ｋ］所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、他のメディアのメディアＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を暗号化した暗号化鍵情報と、前記他のメディアのメディアＩＤに関する情報と本メディアのメディアＩＤに関する情報とから形成された独自ＩＤ情報とが記録されているメディアとした。

［ｌ］前記独自ＩＤ情報を形成するための前記他のメディアのメディアＩＤに関する情報は、前記他のメディアから読み出したそのメディアのメディアＩＤに基づく情報であり、前記独自ＩＤ情報を形成するための前記本メディアのメディアＩＤに関する情報は、前記本メディアから読み出したそのメディアのメディアＩＤに基づく情報であるようにした。

［ｍ］前記独自ＩＤ情報が、前記他のメディアのメディアＩＤと前記本メディアのメディアＩＤとの差分値である差分ＩＤ情報であるようにした。

［ｎ］前記所定のコンテンツ鍵は共通鍵または公開鍵であり、前記ＩＤ鍵は、前記他のメディアのメディアＩＤを用いた共通鍵または前記他のメディアのメディアＩＤを所定の関数により変換した情報を用いた共通鍵であるようにした。

【００１０】まず、図２を用いて本発明の一実施例の構成を説明する。メディアはメディア固有のＩＤが設定され、メディア制御器にセットすることが出来る。メディアは記録再生可能であり、固有のＩＤを設定可能なものであれば、固体メモリーやディスク、テープ等でも良い。但し、ＩＤ情報が所定の耐タンパー性をもつことが条件である。即ち、ＩＤや暗号化に必要な鍵の保管に対して不正に情報を読み出したり、書き換えたりするのが難しい状態になっていることが望ましい。

【００１１】もっとも簡単なものはメモリータイプでこのメモリーカードは所定のメモリー制御器を介してしか、ＩＤや暗号化鍵情報が引き出せない仕組みになっているものが、安全で簡単に作成できる。メモリーカードは、工場生産時にカード毎に固有なＩＤが記録されている。もしくは発行装置により発行される際に、その装置固有のＩＤをＥＥＰＲＯＭなどに記録された後、樹脂封入等で埋めこまれるようになっている。これにより、後からユーザ対応鍵情報が変更できない、つまり不正改ざんできないようにする。メディアには一部のデータのみメディア間のコピーを行うことの出来るメディアバスを有している。

【００１２】メディア制御器はメディアをセットして、ＰＣもしくは専用器などの端末に接続し、メディア内のデータと、端末とのインターフェース機能と、所定のＩＤでのデータの暗号化、復号化機能を有する。メディア制御器は端末側からメモリーの内部を不正にアクセスできない耐タンパー性をもっている。端末は外部にあるコンテンツ情報を配信をするセンター（配信センター）に接続し、課金、認証など所定の手続きを経て、コンテンツデータを受信する。センターとの接続はインターネットなどのネットワークはもちろん、ＩＳＤＮや放送、ケーブルＴＶ、ＰＨＳなどの無線接続でもかまわない。

【００１３】コンテンツ情報は基本的にコンテンツ毎に

15

違う鍵（コンテンツ鍵）で暗号化される。コンテンツはMPEGなどの所定の圧縮方式によって圧縮された後、DESなどの暗号化がなされている。例えばDESの場合、暗号化鍵は６４ビット程度である。データベースとセンターと端末の関係を図１に示す。センターに設置したデータベースで、コンテンツ情報が、コンテンツX1を暗号化鍵G1で暗号化し、また、違うコンテンツX2を暗号化鍵G2で暗号化するものとして管理されている。

【００１４】このセンターには複数の端末がネットワークで接続されている。端末への送信もセキュリティーを考えて公開鍵方式で暗号化して送信する。ここで端末１（T1）の公開鍵をTIPとし、復号鍵をTIDとすると、データベース１に管理されていたコンテンツX1は、暗号化鍵G1で暗号化されEG1(X1)という暗号化コンテンツ情報とされる。暗号化鍵G1は、端末T1に送信するために端末T1の公開鍵TIPを使用して暗号化され、暗号化鍵の情報ET1P(G1)となる。そして、暗号化コンテンツ情報EG1(X1)と暗号化鍵の情報ET1P(G1)との２つの情報を端末１(T1)に送信する。

【００１５】端末１でこのコンテンツ情報を再生するためには、端末１の復号鍵TIDを用いて、暗号化鍵の情報ET1P(G1)を復号し、暗号化鍵G1を得て、その暗号化鍵G1で暗号化コンテンツ情報EG1(X1)を復号し、コンテンツX1を得て、MPEGなどの復号を行うことで再生することが出来るが、ここでは、送信されたデータを端末で再生することなく、すぐに端末に接続されたメディアに記録することを前提とする。ここでは公開鍵を使って端末までのデータ送信を説明したが、これは、共通鍵方式であっても、また他の方式であっても本発明はサポートすることが出来る。

【００１６】次に図３、４、５を用いて本発明の一実施例のコンテンツ情報と鍵情報の受け渡し機能について説明する。

【００１７】最初に配信センターから端末T1側のメディアA（第１のメディア）にコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器にセットする。メディア制御器を端末Ｔ１にセットして、「データ記録モード」にする。誤金、認証など所定の手続きを行う。手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵Gで暗号化されて端末に配信されてくる。

【００１８】即ち、コンテンツX1を暗号化鍵G1で暗号化した暗号化コンテンツ情報EG1(X1)が送信されてくる。また、暗号化鍵G1を端末T1に送信するために、端末T1の公開鍵TIPを使用して暗号化鍵G1を暗号化した暗号化鍵情報ET1P(G1)が端末T1に送信されてくる。端末で復号に使用する鍵はTIDなので、この暗号化鍵情報ET1P(G1)は復号鍵TIDで復号できる。この状態をET1D（G1）と表現する。端末ではこの暗号化鍵情報ET1D（G1）を一度復号鍵T1Dで復号して暗号化鍵G1を得る。

16

【００１９】メディア制御器ではこのデータを受信し、メディアAには暗号化コンテンツ情報EG1(X1)が記録され、同時にメディア制御器はセットされたメディアのIDを認識して、この鍵G1をメディアAの固有のIDであるAという値で再暗号化して暗号化鍵情報EA(G1)得、これをメディアAに記録する。この時点でのメディアAの内容を図３のメディアAのブロックに示す。αは後述する差分ID（独自ＩＤ情報）であり、この時点ではα＝０が記録されている。配信直後のデータ構造を図４（１）に示す。データは先頭に差分ID６４ビット、暗号化鍵情報６４ビット、その後ろに暗号化コンテンツ情報が記録される。

【００２０】次に、メディアAに記録されている暗号化コンテンツ情報を再生する場合を説明する。メディアAをメディア制御器にセットし、メディア制御器を「データ再生モード」とする。暗号化鍵情報EA(G1)を自分のIDであるAにαを加算した値を用いて暗号化鍵G1を復号し、次に暗号化鍵G1を用いて暗号化コンテンツ情報EG1(X)を復号して再生データXを得ることが出来る。ここではα＝０なのでID=Aを用いて復号した場合と等価である。

【００２１】次に、メディアA（第１のメディア）からメディアB（第２のメディア）へデータを譲渡（移動）する場合を説明する。コンテンツの記録されている譲渡元メディアAから譲渡先メディアBに暗号化コンテンツ情報を譲渡する場合、まず、メディア制御器にメディアAをセットする。メディア制御器のモードを「データ移動モード」にする。

【００２２】暗号化鍵情報EA(G1)と譲渡元メディアA（第１のメディア）のIDはメディア制御器のメモリーにデータリンクIDによって対応づけられた形態で一時記録される。これは図３のメディア制御器内メモリーのブロックに示したように、データリンクIDとしてDmという管理ナンバーを一つ選ぶ。これは０から始めて６４ビット以内であれば、シリアルにIDをつけて行くような形態でかまわない。後述するような、データリンクIDを消去する場合に、矛盾なく管理できればどのような打ち方でもかまわない。Dmに関連して、暗号化鍵情報EA(G1)とメディアAのID、及びコンテンツのネームなどが記録される。メディアAには複数のコンテンツが記録される場合も考慮してファイルネーム等、このDmに関連してデータを記録する。

【００２３】暗号化コンテンツ情報EG1(X1)には上記データリンクIDが付加されて、暗号化鍵情報EA(G1)と共に、譲渡先メディアにコピーされる。暗号化コンテンツ情報、暗号化鍵情報EA(G1)はメディアバスを介して高速にメディアBに転送される。このメディアバスは、メディアAとメディアBを物理的に連結して、メディア制御器を介さずにデータ転送を行うものである。このデータ自体に暗号化コンテンツデータのみがこのメディアバス

17

を通過できるようになっているので安全性が高い。暗号化コンテンツ情報構造を図４（２）に示す。メディアAからメディアBに暗号化コンテンツ情報EG1(X1)と暗号化鍵情報EA(G1)とを送信した後、譲渡元のメディアAにある暗号化鍵情報EA(G1)は消去される。また、セキュリティを考えると暗号化コンテンツ情報EG1(X1)も消去することが望ましいが暗号化鍵情報EA(G1)だけ消去されれば、それで暗号の復号はほぼ不可能と考えられる。

【００２４】メディア内部、及びメディア制御器は、外部のバックアップ用メディアや、ＰＣなどの端末などのように外部からの不正なアクセスをすることが不可能であり、情報の消去などのコマンドも確実に実行される。

【００２５】次に、メディア制御器にメディアBをセットする。メディア制御器では、接続された譲渡先メディアBのIDを読み取り、次に、すでに転送されている暗号化コンテンツ情報EG1(X1)に付加されたデータリンクIDのDnを読み取る。また、暗号化鍵情報EA(G1)も同時に読み取る。メディア制御器この時点で「データ移動モード」であるので、差分IDと同じエリアに記録されたデータをデータリンクIDのDnとして認識できる。それをもとにメディア制御器のメモリーからデータリンクIDのDnに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのIDであるID(A)を読み取る。

【００２６】ここで、譲渡先メディアBから読み出したEA(G1)と制御器メモリーから読み出したEA(G1)とを照合する。この鍵情報が一致していなければ以下のプロセスである差分ＩＤを発行しない。即ち、一致していなかった場合、データリンクＩＤが同じでも違ったコンテンツの情報として認識することが出来る。これは、同一のメディアAから複数のメディア制御器を使って、データ移動を行った場合に発生する問題を回避するため、また、不正にコピーしようとしてメディア制御器内メモリーのデータや、メディア内データを改竄しようとした場合に発生する矛盾を発見し、機能を停止するのに効果を発揮する。

【００２７】次に、認証の結果…一致している場合、譲渡先メディアBと譲渡元メディアAのIDの差分値である差分ID、（A-B）値を、譲渡先メディアBに記録する。そして記録後、メディア制御器のメモリーに記録されている前記暗号化鍵情報EA(G1)と譲渡元メディアAのID(A)を消去する。この時点でのメディアBの内容を図３のメディアBのブロックに示す。

【００２８】この消去の動作はメディア間でデータをコピーするのではなく、譲渡（移動）することを可能としている。もともとIDを用いた暗号化は非常に有効であるが、そのメディアでしか再生できないという欠点があったが、外部から操作不可能なメディア制御器内で、暗号化鍵情報とメディアID情報を管理し、コピーと同時に削除することで、ユーザーの使い勝手の良いシステムを提供することが出来るようになる。データ移動後のデータ

18

構造は図４（３）のようになる。移動終了後始めの６４ビットのデータリンクID情報は、差分IDのデータ情報として書き換えられる。

【００２９】次に、メディアBに移動された暗号化コンテンツ情報EG1(X1)を再生する場合を説明する。再生手順は、前記配信後のメディアAを再生する手順と同じである。即ち、このメディアBに記録されている暗号化コンテンツ情報を再生する場合、メディアBをメディア制御器にセットし、メディア制御器を「再生モード」とする。暗号化鍵情報EA(G1)を自分のIDであるB(=α)を加算した値、即ち、B+（A-B）を用いて暗号化鍵G1を復号し、次に暗号化鍵G1を用いて暗号化コンテンツ情報EG1(X1)を復号して再生データX1を得ることが出来る。差分IDであるα＝A-Bなので(B+A)=Aを用いて復号したのと等価であり、再生が可能となる。

【００３０】次に、コンテンツの記録されている譲渡元メディアAからバックアップ用メディアに暗号化コンテンツ情報をコピーする場合について説明する。バックアップメディアとは、メディア制御器に着脱できないメディアを総称して言う。即ちPCのハードディスクや、記録可能な光ディスクなど、本方式の制御器を有していない場合がこれに当たる。ここでは端末PCに接続されたハードディスクをバックアップメディアとする。

【００３１】まず、メディアAをメディア制御器にセットして、メディア制御器を「バックアップ出力モード」とする。メディア制御器をPC端末に接続する。暗号化鍵情報EA(G1)と譲渡元メディアAのIDはメディア制御器のメモリーにデータリンクIDによって対応づけられた形態で記録される。これは図３のメディア制御器内メモリーブロックに示したように、データリンクIDとしてDnという管理ナンバーを一つ選ぶ。このDnに関連して、暗号化鍵情報EA(G1)とメディアAのIDが記録される。暗号化コンテンツ情報EG1(X1)には上記データリンクIDが付加されてメディア制御器を介して暗号化鍵情報EA(G1)と共に端末PCに接続されたハードディスクに転送される。暗号化コンテンツ情報構造を図５に示す。

【００３２】次に、コンテンツの記録されているバックアップ用メディアから譲渡先メディアBに暗号化コンテンツ情報をコピーする場合について説明する。まず、メディアBをメディア制御器にセットして、メディア制御器を「バックアップ入力モード」とする。メディア制御器をPC端末に接続する。バックアップ用メディアに記録されている暗号化コンテンツデータの先頭６４ビットは必ずデータリンクDnである。上記データリンクIDが付加されている暗号化コンテンツ情報EG1(X1)と暗号化鍵情報EA(G1)を譲渡先メディアBにコピーする。

【００３３】メディア制御器は、接続された譲渡先メディアのID（B）を読み取り、暗号化コンテンツ情報EG1(X1)に付加されたデータリンクIDを読み取り、暗号化鍵情報EA(G1)を読み取る。それをもとにメディア制御器

のメモリーからデータリンクIDに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのID（A）を読み取り、譲渡先メディアBから読み出した暗号化鍵情報EA(G1)と制御器メモリーから読み出した暗号化鍵情報EA(G1)とを照合する。

【００３４】認証の結果一致している場合、譲渡先メディアBと譲渡元メディアAのIDの差分値である差分ID、（A-B）値を、譲渡先メディアBに記録する。そして記録後、メディア制御器のメモリーに記録されている前記暗号化鍵情報EA(G1)と譲渡元メディアのID（A）を消去する。このバックアップの動作は図３のメディアAからメディアBへデータを移動した場合と、メディアAから一旦バックアップ用メディアにバックアップし、その後メディアBへ移動したものと等価になる。

【００３５】バックアップメディアからメディアBに移動された暗号化コンテンツ情報EG1(X1)を再生する場合は、すでに説明した前記配信後のメディアAを再生する手順と同じである。即ち、このメディアBに記録されている暗号化コンテンツ情報EG1(X1)を再生する場合、メディアBをメディア制御器にセットし、メディア制御器を「データ再生モード」とする。暗号化鍵情報EA(TID)を自分のIDであるB(=α)を加算した値、即ち、B+（A-B）を用いて暗号化鍵G1を復号し、次に暗号化鍵G1を用いて暗号化コンテンツ情報EG1(X)を復号して再生データXを得ることが出来る。差分IDのα＝A-Bなので、ID=Aを用いて復号したのと等価であり、再生が可能となる。

【００３６】ここでの方式では暗号化コンテンツ情報は公開鍵方式で暗号化されたこととして説明したが、端末の共通鍵Gでセンターから配信され、端末では復号鍵Gを用いても可能である。またメディア固有のIDにて、鍵を暗号化することとして説明したが、IDそのものではなく、所定の関数を用いてIDを変換した情報を用いた鍵で暗号化してもよい。

【００３７】次に、図６を用いて本発明の実施例のブロック図について説明する。最初に配信センターからメディアAにコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器２１にセットする。メディア制御器を端末Ｔ１にセットして、外部インターフェースよりメディア制御器のモード設定部５１に「データ記録モード」を設定する。課金、認証など所定の手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵（コンテンツ鍵）G1で暗号化されて端末Ｔ１に配信されてくる。「データ記録モード」の場合、モード設定部５１は差分ID発生部５２に「０」を発生させるよう指示する。メディア制御器では暗号化コンテンツデータを受信し、暗号化コンテンツデータヘッダー書き込み部５３で、６４ビットの「０」を示すデータをヘッダーに書き込み、暗号化コンテンツ情報EG1(X1)をメディアAのメモリー部３３に記録する。モード設定部５１に「データ記録モード」と設定されているとき、スイッチ２には差分ID発生部５２につながるように切り替えられている。

【００３８】一方メディア側のメディアID発生部３１により発生された信号は、メディア制御器のメディアID読み取り部５４によってメディアのID（A）を検出し、このID（A）でコンテンツの暗号化鍵G1を、鍵暗号化部５５で暗号化して暗号化鍵情報EA(G1)を作成し、メディアのメモリー情報記録消去制御部３２を介してメモリー部３３に記録する。ヘッダーは差分IDを示し、この時点ではひが記録されている。配信直後のデータ構造を図４（１）に示す。データは先頭に差分ID６４ビット、暗号化鍵情報６４ビット、その後ろに暗号化コンテンツ情報が記録される。

【００３９】次に、メディアAに記録されている暗号化コンテンツ情報EG1(X1)を再生する場合を説明する。メディアAをメディア制御器２１にセットし、外部インターフェースよりメディア制御器のモード設定部５１に「データ再生モード」を設定する。メディア制御器２１はメディアAのメモリー部３３から暗号化鍵情報EA(G1)を読み出し、暗号化鍵復号部５６に送信する。またメディア側のメディアID発生部３１により発生された信号は、メディア制御器のメディアID読み取り部５４によってメディアのID（A）を検出し、暗号化復号部５６に送信する。また、メディア制御器２１はメディアのメモリー部３３からメモリー情報記録消去制御部３２を介して暗号化コンテンツ情報EG1(X1)を読み出し、暗号化コンテンツデータヘッダー読み取り部５７に送信する。暗号化コンテンツデータヘッダー読み取り部５７では、先頭にある差分データ６４ビットを読み、スイッチ１を介して差分ID読み取り部５８へ送信される。

【００４０】モード設定部５１によって「データ再生モード」の場合、スイッチ１は差分ID読み取り部５８へ切り替えられている。差分ID読み取り部５８で検出された差分IDは暗号化鍵復号部５６に送信される。暗号化鍵復号部５６では、入力された差分IDとメディアのIDを加算し、IDを生成し、暗号化鍵G1を復号する。ここでは差分ID=０なのでID=Aを用いて復号したのと等価である。復号した暗号化鍵G1は暗号化コンテンツデータ復号部５９に送信される。また、暗号化コンテンツデータヘッダー読み取り部５７でヘッダーから取り出された暗号化コンテンツデータは暗号化コンテンツ復号部５９に送信される。暗号化コンテンツデータ復号部５９では、入力された暗号化コンテンツデータEG1(X1)と暗号化鍵G1によって暗号化コンテンツデータを復号化し、再生データXとして出力する。

【００４１】次に、メディアAからメディアBへデータを譲渡（移動）する場合を説明する。コンテンツの記録されている譲渡元メディアAから譲渡先メディアBに暗号化コンテンツ情報をコピーする場合、まず、メディア制御器２１にメディアAをセットする。外部インターフェー

スよりメディア制御器のモード設定部５１に「データ移動出力モード」を設定する。

【００４２】メディアID発生部３１により発生された信号は、メディア制御器のメディアID読み取り部５４によってメディアのID（A）を検出し、メディア制御器内メモリー６０の記録再生消去制御部６１に送信される。同時に暗号化鍵情報EA(G1)がメディアAから呼び出され、メディア制御器内メモリー６０の記録再生消去制御部６１に送信される。また、データリンクID発生部６２でデータリンクIDが発生されてメディア制御器内メモリー６０の記録再生消去制御部６１に送信される。これら暗号化鍵情報EA(G1)と譲渡先メディアAのIDはメディア制御器のメモリー６０にデータリンクIDによって対応づけられた形態で記録される。後述するような、データリンクIDを消去する場合には消去した情報がデータリンクID発生部に送信され、矛盾なく管理できるIDが発生できるようになっている。

【００４３】データリンクID発生部６２は同時に、暗号化コンテンツデータヘッダー書き込み部５３にもデータリンクIDを送信する。モード設定部５１に「データ移動出力モード」と設定されているとき、スイッチ２は、データリンクID発生部６２につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部５３では、メディアAのメモリー部３３から暗号化コンテンツデータを読み取り、ヘッダーにデータリンクIDを書き込んで、一旦メディアのメモリー３３に戻される。

【００４４】戻された暗号化コンテンツデータは暗号化鍵情報とともにデータ移動用の領域に格納され、メディアバス３４を介して、高速にメディアBに転送される。このメディアバス３４は、メディアAとメディアBを物理的に連結して、メディア制御器を介さずにデータ転送を行う。このデータ自体は暗号化コンテンツデータのみがこのメディアバスを通過できるようになっているので安全性が高い。

【００４５】その後、メディア側のメモリー情報記録消去制御部３２は設定モードが「データ移動出力モード」であることを確認して、譲渡元メディアAにある暗号化鍵情報EA(G1)を消去する。暗号化コンテンツ情報構造を図４（２）に示す。

【００４６】次に、メディア制御器２１にメディアBをセットする。メディア制御器のメディアID読み取り部５４によってメディアのID（B）を検出する。そしてメディアBのメモリー部３２Bにすでに転送記録されている暗号化コンテンツ情報EG1(X1)を暗号化コンテンツデータヘッダー読み取り部５７で送信する。また、メディアBに記録されている暗号化鍵情報EA(G1)を読み取る。

【００４７】モード設定部５１に「データ入力移動モード」と設定されているとき、スイッチ１はデータリンクID読み取り部６３につながるように切り替えられている。データリンクID読み取り部６３では、暗号化コンテンツ情報EG1(X1)のヘッダーについているデータリンクIDを読み取り、メディア制御器内メモリー６０の記録再生消去制御部６１に送信する。記録再生消去制御部６１ではこのデータリンクIDをもとに、メディア制御器のメモリー６０からデータリンクIDのDnに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのIDである ID(A)を読み取る。

【００４８】ここで、譲渡先メディアBから読み出した暗号化鍵情報EA(G1)とメディア制御器メモリー６０から読み出した暗号化鍵情報EA(G1)を暗号化鍵照合部６４に送信し照合する。この鍵情報が一致していなければ以下のプロセスである差分ＩＤを発行しない。照合結果は差分ID発生部５２に送信され、照合結果が一致している場合、ID(A)は差分ID発生部５２に送信される。差分ID発生部５２では入力されたID(A)と、メディアID読み取り部５４によって読み取った譲渡先メディアのID（B）との差を計算し、差分ID（A-B）値を、暗号化コンテンツデータヘッダー書き込み部５３に送信する。

【００４９】モード設定部５１に「データ入力移動モード」と設定されているとき、スイッチ２は差分ID発生部５２につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部５３は対象となるデータリンクIDのついた暗号化コンテンツデータのヘッダーを差分IDの値に書き換える。

【００５０】その後、暗号化コンテンツデータヘッダー書き込み部５３は、書き込み完了の信号をメディア制御器内メモリー６０の記録再生消去制御部６１に出力し、記録再生消去制御部６１は前記暗号化鍵情報EA(G1)と譲渡元メディアのID（A）を消去する。データ移動後のデータ構造は図４（３）のようになる。移動終了後始めの６４ビットのデータリンクID情報は、差分IDのデータ情報として書き換えられる。

【００５１】次に、メディアBに移動された暗号化コンテンツ情報を再生する場合を説明する。再生手順は、前記記信後のメディアAを再生する手順と同じである。即ち、このメディアBに記録されている暗号化コンテンツ情報EG1(X1)を再生する場合、メディアBをメディア制御器２１にセットし、メディア制御器を「データ再生モード」とする。メディア制御器２１はメディアBのメモリー部３３Bから暗号化鍵情報EA(G1)を読み出し、暗号化鍵復号部５６に送信する。またメディア側のメディアID発生部３１Bにより発生された信号は、メディア制御器のメディアID読み取り部５４によってメディアのID（B）を検出し、暗号化復号部５６に送信する。また、メディア制御器２１はメディアBのメモリー部３３Bから暗号化コンテンツ情報EG1(X1)を読み出し、暗号化コンテンツデータヘッダー読み取り部５７に送信する。暗号化コンテンツデータヘッダー読み取り部５７では、先頭にある差分データ６４ビットを読み、スイッチ１を介して差分ID読み取り部５８へ送信される。

【００５２】モード設定部５１によって「データ再生モード」の場合、スイッチ１は差分ID読み取り部５８へ切り替えられている。差分ID読み取り部５８で検出された差分IDは暗号化鍵復号部５６に送信される。暗号化鍵復号部５６では、入力された差分IDとメディアIDを加算し、IDを生成し、暗号化鍵GIを復号する。ここでは差分ID＝A−Bとなっていて ID＝B＋(A−B)、即ちID＝Aを用いて復号したのと等価である。復号した暗号化鍵GIは暗号化コンテンツデータ復号部５９に送信される。また、暗号化コンテンツデータヘッダー読み取り部５７でヘッダーが取り去られた暗号化コンテンツデータEGI(X1)は暗号化コンテンツ復号部５９に送信される。暗号化コンテンツデータ復号部５９では、入力された暗号化コンテンツデータEGI(X1)と暗号化鍵GIによって暗号化コンテンツデータを復号化し、再生データとして出力する。

【００５３】次に、コンテンツの記録されている譲渡元メディアAからバックアップ用メディア７０に暗号化コンテンツ情報をコピーする場合について説明する。まず、メディア制御器２１にメディアAをセットする。外部インターフェースよりメディア制御器のモード設定部５１に「バックアップ出力モード」を設定する。メディア制御器２１を端末Ｔ１に接続する。端末Ｔ１をバックアップ用メディア７０に接続する。

【００５４】メディアID発生部３１により発生された信号は、メディア制御器のメディアID読み取り部５４によってメディアAのID（A）を検出し、メディア制御器内メモリー６０の記録再生消去制御部６１に送信される。同時に暗号化鍵情報がメディアAから呼び出され、メディア制御器内メモリー６０の記録再生消去制御部６１に送信される。

【００５５】また、データリンクID発生部６２でデータリンクIDが発生されてメディア制御器内メモリー６０の記録再生消去制御部６１に送信される。これら暗号化鍵情報EA(G1)と譲渡元メディアAのIDはメディア制御器のメモリー６０にデータリンクIDによって対応づけられた形態で記録される。データリンクID発生部６２は同時に、暗号化コンテンツデータヘッダー書き込み部５３にもデータリンクIDを送信する。モード設定部５１に「バックアップ出力モード」と設定されているとき、スイッチ２は、データリンクID発生部６２につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部５３では、メディアAのメモリー部３３から暗号化コンテンツデータを読み取り、ヘッダーにデータリンクIDを書き込む。データリンクIDが書き込まれた暗号化コンテンツデータEGI(X1)は、メディアAのメモリー部３３から読み出された暗号化鍵情報EA(G1)と共に、端末Ｔ１を介してバックアップメディア７０に送信される。暗号化コンテンツ情報構造を図４（2）に示す。その後、譲渡元メディアAにある暗号化鍵情報EA(G1)はメモリー情報記録消去制御部３２によって消去される。

【００５６】次に、コンテンツの記録されているバックアップ用メディア７０から譲渡先メディアBに暗号化コンテンツ情報を譲渡する場合について説明する。まず、メディアBをメディア制御器２１にセットして、メディア制御器２１を「バックアップ入力モード」とする。メディア制御器のメディアID読み取り部５４によってメディアのID（B）を検出する。次に、アップメディア７０から端末Ｔ１を介して暗号化コンテンツデータEG1(X1)と暗号化鍵情報EA(G1)を読み出し、その暗号化コンテンツデータEG1(X1)と暗号化鍵情報EA(G1)を暗号化コンテンツデータヘッダー書き込み部５３を通過させて、メディアBのメモリー部３３Bに記録させる。

【００５７】続いて、暗号化コンテンツ情報EG1(X1)をメディアBのメモリー部３３Bから暗号化コンテンツデータヘッダー読み取り部５７で送信する。モード設定部５１に「バックアップ入力モード」と設定されているとき、スイッチ１はデータリンクID読み取り部６３につながるように切り替えられている。データリンクID読み取り部６３では、暗号化コンテンツ情報EG1(X1)のヘッダーについているデータリンクIDを読み取り、メディア制御器内メモリー６０の記録再生消去制御部６１に送信する。また、メディアBのメモリー部３３Bから暗号化鍵情報EA(G1)も読み取る。記録再生消去制御部６１ではこのデータリンクIDをもとに、メディア制御器のメモリーからデータリンクIDのDnに対応づけられた暗号化鍵情報EA(G1)と譲渡元メディアのIDであるID(A)を読み取る。

【００５８】ここで、譲渡先メディアBから読み出したEA(G)と制御器メモリー６０から読み出したEA(G1)を暗号化鍵照合部６４に送信し照合する。この鍵情報が一致していなければ以下のプロセスである差分ＩＤを発行しない。照合結果は差分ID発生部５２に送信され、照合結果が一致している場合、ID(A)は差分ID発生部に送信される。

【００５９】差分ID発生部５２では入力されたID(A)と、メディアID読み取り部５４によって読み取った譲渡先メディアのID（B）との差を計算し、差分ID（A−B）値を、暗号化コンテンツデータヘッダー書き込み部５３に送信する。モード設定部５１に「バックアップ入力モード」と設定されているとき、スイッチ２は差分ID発生部５２につながるように切り替えられている。暗号化コンテンツデータヘッダー書き込み部５３は対象となるデータリンクIDのついた暗号化コンテンツデータEGI(X1)のヘッダーを差分IDの値に書き換える。その後、暗号化コンテンツデータヘッダー書き込み部５３は、書き込み完了の信号をメディア制御器内メモリー６０の記録再生消去制御部６１に出力し、記録再生消去制御部６１は前記暗号化鍵情報EA(G1)と譲渡元メディアのID（A）を消去する。

【００６０】データ移動後のデータ構造は図４（3）の

25

ようになる。移動終了後始めの６４ビットのデータリンクID情報は、差分IDのデータ情報として書き換えられる。

【００６１】次に、バックアップメディア７０からメディアBに移動された暗号化コンテンツ情報を再生する場合を説明する。再生手順は、前記配信後のメディアAを再生する手順と同じである。即ち、このメディアBに記録されている暗号化コンテンツ情報ＥG1(X1)を再生する場合、メディアBをメディア制御器２１にセットし、メディア制御器を「データ再生モード」とする。

【００６２】メディア制御器２１はメディアＢのメモリー部３３Ｂから暗号化鍵情報EA(G1)を読み出し、暗号化鍵復号部５６に送信する。また、メディア側のメディアID発生部３１Ｂにより発生された信号は、メディア制御器のメディアID読み取り部５４によってメディアのID（B）を検出し、暗号化鍵復号部５６に送信する。また、メディア制御器はメディアＢのメモリー部３３Ｂから暗号化コンテンツ情報ＥG1(X1)を読み出し、暗号化コンテンツデータヘッダー読み取り部５７に送信する。暗号化コンテンツデータヘッダー読み取り部５７では、先頭にある差分データ６４ビットを読み、スイッチ１を介して差分ID読み取り部５８へ送信される。

【００６３】モード設定部５１によって「データ再生モード」の場合、スイッチ１は差分ID読み取り部５８へ切り替えられている。差分ID読み取り部５８で検出された差分IDは暗号化鍵復号部５６に送信される。暗号化鍵復号部５６では、入力された差分IDとメディアIDを加算し、IDを生成し、暗号化鍵G1を復号する。ここでは差分ID＝A-Bとなっていて ID＝B+(A-B)、即ちID＝Aを用いて復号した場合と等価である。復号した暗号化鍵Gは暗号化コンテンツデータ復号部５９に送信される。また、暗号化コンテンツヘッダー読み取り部５７でヘッダーが取り去られた暗号化コンテンツデータＥG1(X1)は暗号化コンテンツデータ復号部５９に送信される。暗号化コンテンツデータ復号部５９では、入力された暗号化コンテンツデータEG1(X1)と暗号化鍵G1によって暗号化コンテンツデータを復号化し、再生データX1として出力する。

【００６４】このように、本実施例によれば、不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。

【００６５】また、本実施例によれば、１人のユーザーが複数のメデイアを持っていた場合、不正なコピーを防止しつつ、そのメディア間でデータの移動や、一時バックアップをしてから、任意のメデイアにデータを復帰させるシステムを提供できる。

【００６６】さらに、メディアが着脱可能なメディア制御器を有し、メディア制御器にはメモリーを有し、メディア間の暗号化コンテンツ情報ＥG1(X1)の移動を行う場合には、暗号化鍵情報EA(G1)をメモリーに一時記録して移動終了後暗号化鍵情報EA(G1)を消去し、バックアップ用メディアに移動する場合には、次にバックアップ用メディアから復帰するまで暗号化鍵情報EA(G1)をメモリーに一時記録して復帰時に暗号化鍵情報EA(G1)を消去するようにしたので、一時バックアップをしてから、任意のメディアにデータを復帰させる時などに、不正な複数メディアへのコピーを防止しつつ、メディア間のデータ移動を自由に行うことが可能となる。

【００６７】また、メディア制御器内メモリーに一時記録した移動元メディアの暗号化鍵情報EA(G1)と、移動先のメディア内から読み出した移動元メデイアの暗号化鍵情報EA(G1)とが同一か否かを認証し、同一と認証したときのみ差分IDを生成し記録するようにしたので、同一のメデイアAから複数のメデイア制御器を使って、データ移動を行った場合に発生する問題を回避できる。さらには、この認証機能は、不正にコピーしようとしてメディア制御器内メモリーのデータや、メデイア内データを改ざんしようとした場合に発生する矛盾を発見し、機能を停止するのに効果を発揮する。

【００６８】

【発明の効果】本発明によれば、不正なコピーを防止しつつ、コンテンツデータの記録されたメディアをユーザー間で譲渡することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。

【００６９】また、本発明によれば、1人のユーザーが複数のメデイアを持っていた場合、そのメデイア間でデータの移動や、一時バックアップをしてから、不正なコピーを防止しつつ、任意のメデイアにデータを復帰させるシステムを提供できる。

【図面の簡単な説明】

【図１】一実施例に用いるデータ配信時の暗号化を説明するための図である。

【図２】一実施例の構成を示す図である。

【図３】一実施例の機能説明図である。

【図４】一実施例のメデイア内のデータ構造図である。

【図５】一実施例のバックアップ用メデイア内のデータ構造図である。

【図６】一実施例の詳細構成を示すブロック図である。

【符号の説明】

２１　メディア制御器（コンテンツ情報処理装置、コンテンツ情報復元装置）

５２　差分ＩＤ発生部（独自ＩＤ情報形成手段）

５３　暗号化コンテンツデータヘッダー書き込み部（データリンクＩＤ書き込み手段）

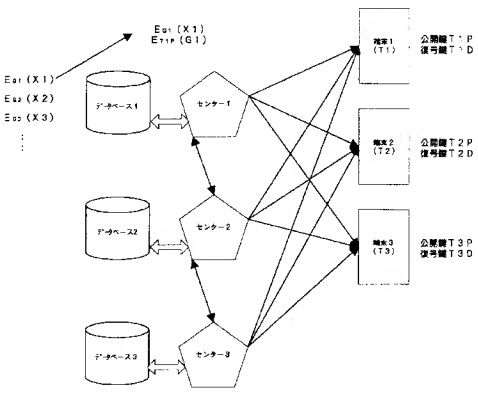
５６　暗号化鍵復号部（コンテンツ鍵復元手段）

５９　暗号化コンテンツデータ復号部（コンテンツ情報復元手段）

６０　メディア制御器内メモリ（第１のメディアのメディアＩＤに関する情報を一時記録するメモリ）
６１　記録再生消去制御部（消去手段、メモリ読み出し手段）
６４　暗号化鍵認証部（暗号化鍵情報照合手段）
７０　バックアップ用メディア

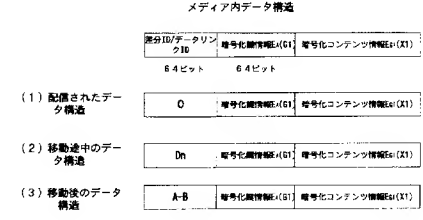
【図１】

図1



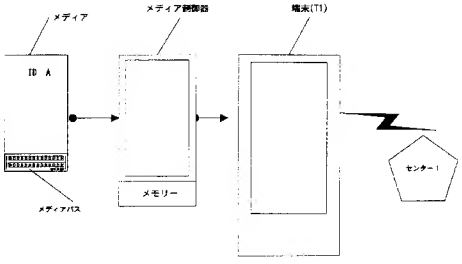
【図４】

図４



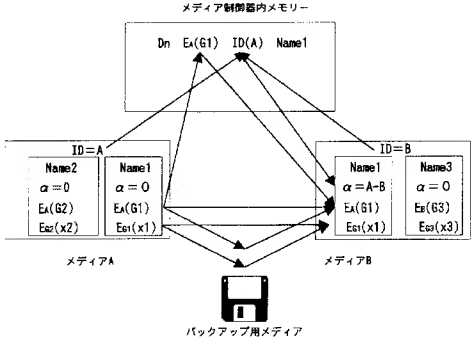
【図２】

図２


メディア
メディア制御器
端末(T1)
ID A
メモリー
センター1
メディアバス

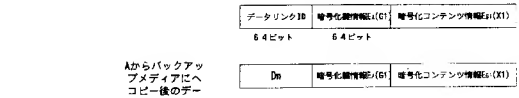
【図３】

図３


メディア制御器内メモリー
Dn EA(G1) ID(A) Name1
ID＝A
Name2
α＝0
EA(G2)
EB2(x2)
Name1
α＝0
EA(G1)
EB1(x1)
ID＝B
Name1
α＝A-B
EA(G1)
EB1(x1)
Name3
α＝0
EB(G3)
EB3(x3)
メディアA
メディアB
バックアップ用メディア

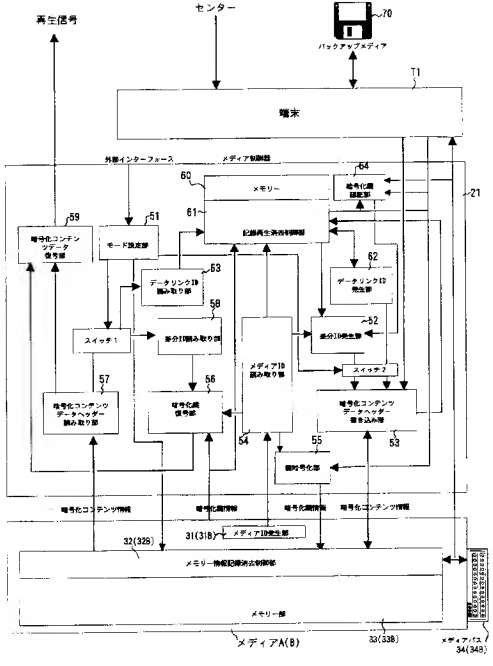
【図５】

図５


バックアップ用メディア内データ構造
データリンクID
暗号化鍵情報Ek(G1)
暗号化コンテンツ情報Ek1(X1)
６４ビット
６４ビット
Aからバックアップメディアにコピー後のデータ構造
Dn
暗号化鍵情報Dn(G1)
暗号化コンテンツ情報Ek1(X1)

【図６】

図６


センター
再生信号
70
バックアップメディア
T1
端末
外部インターフェース
メディア制御部
60
メモリー
64
暗号化鍵
識別子
21
59
暗号化コンテンツデータ
復号部
51
モード設定部
61
記録再生消去制御部
63
データリンクID
読み取り部
62
データリンクID
作成部
58
スイッチ1
著作ID読み取り部
52
著作ID作成部
メディアID
読み取り部
スイッチ2
57
暗号化コンテンツデータヘッダー
読み取り部
56
暗号化鍵
復号部
54
55
53
暗号化コンテンツデータヘッダー
書き込み部
個別暗号部
暗号化コンテンツ情報
暗号化鍵情報
暗号化鍵情報
暗号化コンテンツ情報
31(31B)
メディアID作成部
32(32B)
メモリー情報記録消去制御部
メモリー部
メディアA(B)
33(33B)
メディアバス
34(34B)